Deutscher Bundestag **Drucksache 14/9683**
14. Wahlperiode 03. 07. 2002

Antrag

**der Abgeordneten Jörg Tauss, Monika Griefahn, Hermann Bachmaier, Klaus Barthel (Starnberg), Hans-Werner Bertl, Kerstin Griese, Hubertus Heil, Ulrich Kelber, Ernst Küchler, Klaus Lennartz, Wilhelm Schmidt (Salzgitter), Lydia Westrich, Dr. Peter Struck und der Fraktion der SPD
sowie der Abgeordneten Grietje Bettin, Kerstin Müller (Köln), Rezzo Schlauch und der Fraktion BÜNDNIS 90/DIE GRÜNEN**

Sichere Informations- und Kommunikationsinfrastrukturen gewährleisten

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Mit der zunehmenden Bedeutung elektronischer Informations- und Kommunikationsinsfrastrukturen für alle gesellschaftlichen Bereiche wächst zugleich das Bewusstsein um die neuen Gefahren, die mit den spezifischen Merkmalen elektronischer Datenverarbeitung in globalen Netzwerken einher gehen. Der unerlaubte Zugriff auf vertrauliche Daten und Kommunikation, das unerlaubte Eindringen in geschlossene Netzwerke (Hacking), die Funktionsbeeinträchtigung der technischen Systeme (Denial of Service Attacks) bis hin zu Terrorakten oder der regelrechten Kriegsführung im Netz (Cyber Terror oder Cyber War) machen deutlich, dass eine umfassende informationstechnische Sicherheit (IT-Sicherheit) zunehmend zur Voraussetzung für eine positive Entwicklung der Informationsgesellschaft wird. Dies gilt umso mehr, je stärker auch sensible, vertrauliche oder folgenreiche Informationen, Kommunikationen und Transaktionen über elektronische Informations- und Kommunikationsinfrastrukturen (IuK) ausgetauscht, geführt oder abgewickelt werden. Die hinreichende Sicherheit und Verfügbarkeit dieser IuK-Infrastrukturen ist nicht allein ein Frage für den elektronischen Geschäftsverkehr (E-Commerce) oder für elektronische Dienstleistungen moderner Verwaltungen und Behörden (E-Government), sie ist vor allem auch für den modernen Staat eine zentrale Aufgabe einer zukunftsfähigen Vorsorge- und Infrastrukturpolitik. Die zentralen Einrichtungen und Institutionen des Bundes und der Länder sowie die lebenswichtigen Infrastruktureinrichtungen sind auf sichere und hochverfügbare elektronische IuK-Infrastrukturen angewiesen. Da die IuK-Infrastruktur ein integraler Bestandteil der lebenswichtigen kritischen Infrastrukturen ist, ist ihre Sicherheit und Verfügbarkeit für einen modernen Staat von besonderer Bedeutung.

Der Deutsche Bundestag begrüßt die zahlreichen Initiativen im Bund, in den Ländern, auf europäischer und auf internationaler Ebene, die ein höheres Sicherheitsbewusstsein und eine verbesserte IT-Sicherheit zum Ziel haben. Sowohl in der EU-Initiative „e-Europe“ der EU-Kommission als auch im Aktionsprogramm der Bundesregierung „Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts“ genießt IT-Sicherheit zu Recht einen hohen Stellenwert. Der Deutsche Bundestag begrüßt die OECD-Initiative eine neue „Kultur der Sicherheit“ in elektronischen Netzwerken zu begründen.

Die Sicherheit und Verfügbarkeit kritischer elektronischer IuK-Infrastrukturen ist für den modernen Staat unabdingbar. Der Deutsche Bundestag begrüßt, dass der Bundesregierung mit dem Informationsverbund Berlin-Bonn (IVBB) bereits ein eigenes, breitbandiges und logisch vom Internet getrenntes eigenständiges Netzwerk zur Verfügung steht. Dieses ist vor äußeren Hackerangriffen oder Viren ebenso besonders geschützt, wie die Benutzer gegenseitig voreinander vor internen Angriffen. Die wenigen Übergänge zum offenen Netzwerken sind sehr gut abgesichert und werden ständig kontrolliert (Firewall, Intrusion Detection, Virenscanner usw.). Angeschlossen an den IVBB sind neben den Bundesministerien, dem Deutschen Bundestag und dem Bundesrat ebenfalls u. a. alle Sicherheitsbehörden, die obersten Gerichte und auch das Robert Koch-Institut. Zusätzlich sind die wichtigsten Einrichtungen des Bundes im IVBB darüber hinaus auch physikalisch vom globalen Netzwerk getrennt, d. h. es existiert eine eigene Netzinfrastruktur mit eigenständiger IuK-Technik. Der gesamte Sprach- und Datenverkehr (Telefonie, Telefax, E-Mail, Internet-Zugang, Videokonferenzen usw.) der Bundesministerien, des Deutschen Bundestages und auch des Bundesrates werden allein über dieses besondere Netzwerk abgewickelt. Der Deutsche Bundestag begrüßt, dass auch die Bundesländer sich für ihren Datenverkehr in einem eigenen Verbund zusammengeschlossen haben (TESTA Deutschland). Auch diese Netzinfrastruktur genügt hohen Sicherheitsanforderungen und ist ebenfalls logisch von andern Netzwerken getrennt. Dazu besitzt es eine Querverbindung zum IVBB, so dass die Bundesländer bzw. die angeschlossenen Landesministerien auch aus dem IVBB heraus über TESTA erreichbar sind.

Ziel dieser Sicherheits- und Vorsorgemaßnahmen ist es, die Funktionsfähigkeit der IuK-Infrastrukturen und Verfügbarkeit der IuK-Dienste nicht nur im Regelbetrieb, sondern vor allem auch in Notfallsituationen zu gewährleisten. Besonders hervorzuheben ist, dass der IVBB im Falle eines tatsächlichen erfolgreichen Angriffs vom „Rest der Welt“ abgekoppelt werden und völlig eigenständig betrieben werden kann. Zur IT-Sicherheit gehört ebenfalls, dass wichtige Systeme mehrfach vorhanden sind (Redundanz) und partielle Ausfälle nie zu einem völligen Ausfall des IuK-Systems führen können. Der Deutsche Bundestag begrüßt, dass die Bundesregierung mit dem Sicherheitspaket diese Redundanz der Systemkomponenten noch einmal erhöht und die Verfügbarkeit verbessert hat. Der IVBB unterliegt ständigen Sicherheits- und Funktionsüberprüfungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), hinzu kommen sichere Übergänge zu offenen Netzen und wiederholte Penetrationstests (simulierte Angriffsversuche durch Sicherheitsfachleute). Es sollte erwähnt werden, dass bisher kein erfolgreicher Fall eines unerlaubten Eindringens in das bzw. Schädigens des IVBB bekannt ist.

Aber nicht nur elektronische, auch andere Infrastrukturen können über oder mittels elektronischer IuK-Systeme angegriffen werden. Der Deutsche Bundestag begrüßt vor diesem Hintergrund die Einsetzung der interministeriellen Arbeitsgruppe KRITIS durch die Bundesregierung. Diese hat die Aufgabe, eine Gefährdungsanalyse zu erstellen und mögliche Bedrohungsszenarien zu bestimmen. Dazu gehört neben der Verfügbarkeit elektronischer IuK-Infrastrukturen ebenfalls, weitere kritische Infrastrukturen, die über oder mittels elektronischer IuK-Netzwerke potentiell angreifbar sind (wie beispielsweise die Wasser- und Energieversorgung oder das Verkehrssystem), auf mögliche Schutzlücken hin zu prüfen. Vorgesehen ist, denkbare Lösungsansätze für identifizierte Schutzlücken sowie für die Schadensbegrenzung im Falle eines tatsächlichen Angriffs zu entwickeln. Von besonderer Bedeutung für die Prävention ist hierbei der weitere Auf- und Ausbau eines effektiven Frühwarnsystems sowie entsprechender Analysekapazitäten. Nicht förderlich ist es aus Perspektive der informationstechnischen Sicherheit allerdings, alle elektronischen IuK-Netze der bestehenden kritischen Infrastrukturen in einem gesonderten, einheitlichen

und zentralen Netz zusammenfassen zu wollen. Zentralisierte Lösungen bergen allein aufgrund ihrer hohen technischen und organisatorischen Komplexität besondere Risiken (Vielfalt der Gefährdungsdimensionen, Anzahl der Nutzungsberechtigten usw.) und erhöhen sogar die Gefährdung, da Funktionsbeeinträchtigungen infolge von technischen Störungen oder von Angriffen sich innerhalb homogener Netzstrukturen kaum lokal begrenzen lassen. Dezentrale Lösungen, wo überschaubare und technisch handhabbare gesicherte Netzwerke miteinander über besonders gesicherte Schnittstellen Daten austauschen, bieten allein von der Grundkonzeption her bereits einen deutlichen Sicherheitsgewinn. Zentralisierung und der Aufbau einer Parallel-Infrastruktur für kritische IuK-Netze wäre eine ineffiziente Verschwendung von Ressourcen, die nicht nur keinen tatsächlichen Sicherheitsgewinn, sondern darüber hinaus sogar zusätzliche Sicherheitsprobleme produzieren würde.

Der Deutsche Bundestag begrüßt, das die Bundesregierung mit der Einrichtung der „Task Force Sicheres Internet“ ihre Bemühungen intensiviert hat, um auch außerhalb der Regierungsnetze die Sicherheit des Internets insgesamt zu erhöhen. In hochdynamischen und globalen Netzwerken kommt dem technisch implementierten Systemschutz und Selbstschutz der Nutzer eine besondere Bedeutung zu. Unter diesen Rahmenbedingungen bildet die von der Bundesregierung beschlossene Nicht-Regulierung kryptographischer Hilfsmittel – die so genannte Kryptofreiheit – eine unverzichtbare Voraussetzung für verlässliche Sicherheitskonzepte. Ebenso besitzt nach Ansicht vieler Experten das so genannte Open Source-Entwicklungskonzept erhebliche Potentiale hinsichtlich einer verbesserten IT-Sicherheit. Das politische Ziel, solche Lösungen und Technologien zu fördern, stellt daher einen Beitrag zum wirkungsvolleren Schutz vor den Verwundbarkeiten der Informationsgesellschaft dar. Ziel muss es sein, sowohl dass Bewusstsein für die Sicherheit elektronischer IuK-Infrastrukturen zu erhöhen als auch sichere technische System- wie Selbstschutzkonzepte zu ermöglichen und zu fördern.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. die vorgesehenen Maßnahmen des Aktionsprogramms der Bundesregierung und der Initiative e-Europe schnellstmöglich umzusetzen und die Schaffung einer internationalen „Kultur der Sicherheit“ zu fördern;
2. den IVBB weiterhin auf dem Stand der Technik weiterzuentwickeln und zu prüfen, inwieweit weitere sensible Einrichtungen und Institutionen ebenfalls angeschlossen werden können;
3. das Sicherheitskonzept der Regierungsnetze weiterhin fortlaufend zu aktualisieren und flexibel an neue oder veränderte Bedrohungsszenarien anzupassen und hierbei wo möglich dezentralen den Vorzug vor zentralisierten Lösungen zu geben;
4. weiterhin die Freiheit von kryptographischen Hilfsmitteln als Voraussetzung für einen effektiven Selbst- und Systemschutz zu unterstützen;
5. zu prüfen, inwieweit die Entwicklung und Implementierung von Open Source-Software weiterhin gefördert werden kann;
6. zu prüfen, inwieweit kritische Infrastrukturen trotz der hohen Sicherheitsstandards durch oder über offene elektronische IuK-Netzwerke beeinflusst oder gefährdet werden können und diesbezüglich Lösungsstrategien vorzulegen.

Berlin, den 3. Juli 2002

Dr. Peter Struck und Fraktion
Kerstin Müller (Köln), Rezzo Schlauch und Fraktion



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon (02 28) 3 82 08 40, Telefax (02 28) 3 82 08 44
ISSN 0722-8333